EXHIBIT A

2122-CC00411 - DARNELL CRAWFORD ET AL V THYSSENKRUPP MATERI ET AL (E-CASE)

Click here to eFile on Case
Click here to Respond to Selected Documents

Sort Date Entries: (•) Descending ( ) Ascending

Display Options: All Entries

03/15/2021 ☐ **Entry of Appearance Filed**

Entry of Appearance; Electronic Filing Certificate of Service.

Filed By: AARON DAVID HABER

On Behalf Of: DARNELL CRAWFORD JR, MICHAEL DEW

03/12/2021 ☐ **Memorandum Filed**

Memorandum Filing Return of Service on Defendant ThyssenKrupp Supply Chain NA, INC; Affidavit of Service.

Filed By: JOHN FRANCIS GARVEY JR

☐ **Memorandum Filed**

Memorandum Filing Return of Service on Defendant ThyssenKrupp Materials NA, Inc; Affidavit of Service.

Filed By: JOHN FRANCIS GARVEY JR

03/08/2021 ☐ **Jury Trial Scheduled**

Scheduled For: 08/09/2021; 9:00 AM ; MICHAEL FRANCIS STELZER; City of St. Louis

03/04/2021 ☐ **Certificate of Service**

Certificate of Service of First Interrogatories and First Request for Production to ThyssenKrupp Supply Chain.

Filed By: JOHN FRANCIS GARVEY JR

On Behalf Of: DARNELL CRAWFORD JR, MICHAEL DEW

☐ **Certificate of Service**

Certificate of Service of First Interrogatories and First Request for Production to Defendant ThyssenKrupp Materials.

Filed By: JOHN FRANCIS GARVEY JR

On Behalf Of: DARNELL CRAWFORD JR, MICHAEL DEW

☐ **Summons Issued-Circuit**

Document ID: 21-SMCC-1415, for THYSSENKRUPP SUPPLY CHAIN SERVICES NA, INC..

☐ **Summons Issued-Circuit**

Document ID: 21-SMCC-1414, for THYSSENKRUPP MATERIALS NA, INC.

02/25/2021 ☐ **Filing Info Sheet eFiling**

Filed By: JOHN FRANCIS GARVEY JR

☐ **Note to Clerk eFiling**

Filed By: JOHN FRANCIS GARVEY JR

☐ **Pet Filed in Circuit Ct**

Class Action Petition; Exhibit A.

Filed By: JOHN FRANCIS GARVEY JR

On Behalf Of: DARNELL CRAWFORD JR, MICHAEL DEW

☐ **Judge Assigned**

IN THE CIRCUIT COURT OF THE CITY OF ST. LOUIS
STATE OF MISSOURI

DARNELL CRAWFORD, 4747 Washington Ave. Apt. A Saint Louis, Missouri 63108 -and- **MICHAEL DEW**, 1236 Senate Drive Spanish Lake, Missouri 63138 *Plaintiffs,* **VS.** **THYSSENKRUPP MATERIALS NA, INC.,** Serve: CSC-Lawyers Incorporating Service Company 221 Bolivar Street Jefferson City, MO 65101 -and- **THYSSENKRUPP SUPPLY CHAIN SERVICES NA, INC.,** Serve: CSC-Lawyers Incorporating Service Company 221 Bolivar Street Jefferson City, MO 65101 *Defendants,*	**CASE NO.** **JURY TRIAL DEMANDED**

CLASS ACTION PETITION

Plaintiffs Darnell Crawford and Michael Dew (hereinafter, collectively "Plaintiffs") on behalf of themselves and the proposed class defined below allege as follows:

NATURE OF THE ACTION

1. This case is about the failure of an employer, ThyssenKrupp Materials NA, Inc. and ThyssenKrupp Supply Chain Services NA, Inc.[1] (collectively, "ThyssenKrupp" or "Defendants"), to safeguard its employees' personally identifiable information ("PII").

2. On or about December 28, 2020, ThyssenKrupp's servers and workstations were hijacked in a ransomware attack that compromised the PII of its current and former employees (the "Data Breach"). ThyssenKrupp notified victims of the Data Breach one month later, on January 28, 2021.

3. The compromised PII includes but is not limited to current and former employees' names, addresses, Social Security numbers, dates of birth, direct deposit information, health information and contact information.

4. Plaintiffs are employees of Defendants that are victims of Defendants' negligence and insufficient data security practices. Plaintiffs have suffered a tangible and concrete injury-in-fact.

5. Accordingly, Plaintiffs, on their own behalf and on behalf of a class of similarly situated individuals, bring this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendants' possession.

THE PARTIES

6. Plaintiff Darnell Crawford is a natural person and citizen of the state of Missouri, residing in St. Louis City .

7. Plaintiff Michael Dew is a natural person and citizen of the state of Missouri, residing in St. Louis County.

[1] ThyssenKrupp Supply Chain Services NA, Inc. is the Division of ThyssenKrupp Materials NA, Inc. that Plaintiffs work for.

8. Defendant ThyssenKrupp Materials NA, Inc. is a foreign corporation with its principal place of business in Southfield, Michigan.

9. Defendant ThyssenKrupp Supply Chain Services NA, Inc. is a foreign corporation with its principal place of business in Southfield, Michigan.

JURISDICTION AND VENUE

10. This court is vested with subject-matter jurisdiction pursuant to Mo. Stat. § 478.070.

11. This Court has personal jurisdiction over Defendants because: (a) they are registered to, and in fact do, conduct substantial and not isolated activity within Missouri; (b) they have sufficient minimum contacts in Missouri, or otherwise intentionally avail themselves of Missouri through the promotion, sale, marketing and distribution of its services, to render the exercise of jurisdiction by this Court proper and necessary; and (c) it operates an office at 140 Enterprise Drive, Wentzville, Missouri 63385, and this action arises from Plaintiffs' employment with Defendants at that location.

12. Venue is proper in this Court pursuant to Mo. Stat. § 508.010(4) because Plaintiffs' injury first occurred in St. Louis City. Due to ThyssenKrupp's negligent and or reckless failure to properly protect and maintain Plaintiffs' information Plaintiffs' injuries and damages occurred in St. Louis City.

COMMON FACTUAL ALLEGATIONS

13. ThyssenKrupp Materials NA, Inc. is a leading North American distributor of production materials and provider of integrated supply chain solutions, which employs more than four-thousand employees at more than seventy-five service centers throughout North America.[2]

14. As a condition of employment, ThyssenKrupp requires its employees to entrust it with certain personal information. In its ordinary course of business, ThyssenKrupp maintains that PII, including the names, addresses, Social Security numbers, dates of birth, direct deposit information, health information and contact information of its employees.

15. Plaintiffs and members of the proposed Class, as ThyssenKrupp's current and former employees, relied on it to keep their PII confidential and securely maintained.

16. On or about February of 2016, ThyssenKrupp's parent company, thyssenkrupp Aktiengesellschaft's systems were compromised in a cyber-attack perpetrated by hackers presumed to be from the Southeast Asian region.[3]

17. On or about September of 2020, the Conti ransomware group leaked documents from thyssenkrupp Aktiengesellschaft's Canadian elevator subsidiary, as part of a ransomware attack.[4]

---

[2] *See Company Overview – thyssenkrupp Materials NA*, THYSSENKRUPP MATERIALS NA, INC., *available at* https://www.thyssenkrupp-materials-na.com/company (last visited Feb. 18, 2021).
[3] *See Statement on the cyber-attack at thyssenkrupp*, THYSSENKRUPP AG, *available at* https://www.thyssenkrupp.com/en/newsroom/dataprotection (last visited February 18, 2021).
[4] *See* Ax Sharma, *ThyssenKrupp suffers ransomware attack for the third time*, SECURITY REPORT LTD., (FEB. 1, 2021), *available at* https://securityreport.com/thyssenkrupp-suffers-ransomware-attack-for-the-third-time/ (last visited Feb. 18, 2021).

18. In December of 2020, the Mount Locker ransomware group started publishing data it had procured from ThyssenKrupp System Engineering, another subsidiary of thyssenkrupp Aktiengesellschaft, via a second ransomware attack.[5]

19. On or about December 28, 2020, ThyssenKrupp's servers and workstations were hijacked in a third ransomware attack by the NetWalker ransomware group that compromised the PII of its current and former employees (the "Data Breach").[6] ThyssenKrupp notified victims of the Data Breach one month later, on January 28, 2021.

20. According to ThyssenKrupp's written notice of the Data Breach, it "was the victim of a ransomware attack encrypting [its] servers and workstations." (hereinafter the "Notice Letter", a copy of Plaintiff Michael Dew's Notice Letter is annexed hereto as Plaintiffs' *Exhibit A*). The Notice Letter is sparse on details, but although ThyssenKrupp claims to have "taken immediate action to investigate and isolate the attack and secure [its] IT environment… The threat actor had access to the data in [its] system which could include HR information about [its] current and former employees… [which included] one or more of the following: name, address, social security number, birthdate, direct deposit information, payroll information, health information, and contact information."[7]

21. The Notice Letter encouraged ThyssenKrupp employees to "remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring [their] credit reports for unauthorized activity…" and to "monitor [their] personal accounts and change [their] passwords, particularly if [they] logged into any sensitive accounts (e.g., banking or financial institution accounts) from a tk Materials' workstation."[8]

---

[5] *See ibid.*
[6] *See ibid.*
[7] (Pls.' Ex. A).
[8] *Ibid.*

22. Plaintiffs and members of the Proposed Class are victims of the Data Breach who relied on ThyssenKrupp to keep their PII confidential and securely maintained.

23. The PII stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach—most notably name, date of birth and social security number—is difficult, if not impossible, to change.

24. PII data for sale is so valuable because PII is so broad, and it can therefore be used for various criminal activities, such as creating fake IDs, applying for loans, opening credit cards, applying for government benefits, and if PII is given to law enforcement during the course of an arrest, it is possible that the putative class members could become embroiled in the criminal justice system.

25. ThyssenKrupp was negligent in safeguarding the victims' PII because ThyssenKrupp had repeated warnings and alerts of the increasing risk of ransomware attacks—especially since it failed to prevent two other ransomware attacks shortly before the Data Breach occurred.

26. Over the past several years, data breaches in general, and ransomware attacks in particular, have become alarmingly commonplace. In 2018, the prevalence of ransomware attacks increased by 350%.[9] In 2019, the manufacturing industry—ThyssenKrupp's industry—was the second highest reported "mark" among all major sectors for ransomware attacks.[10]

[9] *2020 Ransomware Statistics, Data, & Trends*, PURPLESEC LLC, *available at* https://purplesec.us/resources/cyber-security-statistics/ransomware/#Industry (last accessed Feb. 19, 2021).
[10] *Ibid.*

27. To this day, ransomware attacks constitute the number one cybersecurity threat for industries throughout the United States and beyond.[11]

28. The most common vector for deploying ransomware is the use of spam/phishing emails.[12] The Notice Letter does not specify how the Data Breach occurred, so it is highly likely that it happened from a phishing email.

29. Companies can mount two primary defenses to phishing scams: employee education and technical security barriers.

30. Employee education is the process of adequately making employees aware of common phishing attacks and implementing company-wide policies requiring the request or transfer of sensitive passwords and other credentials to known recipients through secure sources. Employee education and secure file-transfer protocols provide the easiest method to assist employees in properly identifying fraudulent e-mails and preventing unauthorized access to PII.

31. From a technical perspective, companies can also greatly reduce the flow of phishing e-mails by implementing certain security measures governing e-mail transmissions. Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send emails on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication, which serves to block email streams that have not been properly authenticated.

32. Upon information and belief, ThyssenKrupp failed to adequately train its employees on even the most basic of cybersecurity protocols, including:

---

[11] *See* Jason Firch, *10 Cyber Security Trends You Can't Ignore in 2021*, PURPLESEC LLC, *available at* https://purplesec.us/cyber-security-trends-2021/#Ransomware (last accessed Feb. 19, 2021).
[12] *Ransomware Statistics, supra*, n.8.

a. How to detect phishing emails and other scams, including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

b. Effective password management and encryption protocols for internal and external emails;

c. Avoidance of responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to computers and files containing sensitive information;

e. Implementing guidelines for maintaining and communicating sensitive data; and

f. Protecting sensitive employee information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients.

33. The Data Breach was caused by ThyssenKrupp's violation of its obligation to abide by best practices and industry standards concerning the security of its computer and email systems. ThyssenKrupp failed to comply with security standards and allowed its employees' PII to be stolen by failing to implement security measures that could have prevented or mitigated the Data Breach.

The Data Breach and Notice Letter

34. ThyssenKrupp admitted to the Data Breach on or about January 28, 2021 in the Notice Letter.

35. ThyssenKrupp identified only the following actions it undertook to mitigate and remediate the harm caused by its Data Breach:

> We take the security of personal information very seriously, and we want to assure you that we've already taken steps to prevent a reoccurrence by increasing the monitoring of our networks, further improving access controls and hardening our systems.

ThyssenKrupp did not specify precisely what further steps it took to improve its access controls and harden its systems.

PII was Stolen and Defendants Immediately Recognized the Risk of Identity Theft

36. The gravamen of this lawsuit is that ThyssenKrupp failed to keep Plaintiffs' and the Class Members' PII confidential, whether knowingly and willfully or negligently, as required by law, and that Plaintiffs and the Class Members have suffered legally cognizable concrete and tangible injury as a result. There is a high and substantial likelihood that Plaintiffs' and the Class Members' stolen PII is being misused by cyber-criminals right now, and that misuse will be ongoing and without authorization. Plaintiffs and Class Members therefore have incurred significant out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud.

37. ThyssenKrupp recognized the actual imminent harm and injury that flowed from the Data Breach, so it recommended that Plaintiffs and Class Members "monitor [their] personal accounts and change [their] passwords, particularly if [they] logged into any sensitive accounts (e.g., banking or financial institution accounts) from a tk Materials' workstation…"[13]

38. ThyssenKrupp also offered employees complimentary credit reporting and identify-theft protection services.

39. Even with complimentary identity-theft protection, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII has still substantially increased as a result of the Data Breach.

[13] (Pls.' Ex. A).

40. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and Class Members' PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and Class Members' financial accounts.

41. The act of stealing or improperly accessing Plaintiffs' and the Class Members' PII, and the cyber-criminals' purpose in stealing Plaintiffs' and the Class Members' PII, was to commit additional illegal acts and crimes, such as generating fraudulent charges with Plaintiffs' and the Class Members' financial accounts, gaining unauthorized access to their internet accounts, opening unauthorized financial accounts, and perpetrate identity theft, among other criminal activity. Theft of PII necessarily implies harm because the misuse of data is the only plausible explanation for the Data Breach.

42. This type of injury and harm, including actual fraud, is directly traceable to the Data Breach. This harm is not just possible, not just certainly impending, it has happened and is *ongoing*, and all Class Members are in imminent and immediate danger of being further subjected to this injury.

43. The ramifications of ThyssenKrupp's failure to keep its employees' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

44. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying information" as "any name or number that may be used, alone or

[14] 17 C.F.R. § 248.201 (2013). To be clear, Plaintiffs do not bring the instant action pursuant to any federal law.

in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[15]

45. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

46. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[16]

47. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect: An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

48. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[15] *Ibid.*

[16] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMIN., *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited April 11, 2018).

49. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center: "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

50. Based on the foregoing, the information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach such as those that occurred at Target and Home Depot. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach is difficult, if not impossible, to change—Social Security number, name, employment information, income data, etc.

51. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[18]

52. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police during an arrest.

53. The fraudulent activity resulting from the Data Disclosure may not come to light for years.

---

[17] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back,* NPR, (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackershas-millions-worrying-about-identity-theft, (last visited April 11, 2018).

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD, (Feb. 6, 2015), *available at* http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html, (last visited April 11, 2018).

54. Despite all of the publicly-available knowledge of PII being compromised and alerts regarding the phishing email scam perpetrated, ThyssenKrupp's approach to maintaining the privacy of its employees' PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

55. ThyssenKrupp has failed to compensate Plaintiffs and Class Members victimized in this Data Breach. Upon information and belief, ThyssenKrupp has not offered to provide assistance or compensation for the costs and burdens—current and future—associated with the identity theft and fraud resulting from the Data Breach. ThyssenKrupp has not offered victims of the Data Breach any assistance in dealing with the IRS, the state tax agencies, or any of the three major credit-reporting agencies.

56. It is incorrect to assume that reimbursing a victim of the Data Breach for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[19]

57. As a result of ThyssenKrupp's failure to prevent the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise, publication and/or theft of their PII;

[19] *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUSTICE (Dec. 2013) at *10, 11, available at* https://www.bis.gov/content /pub/pdf/vitl2.pdf (last visited April 11, 2018).

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII;

h. The continued risk to their PII, which remains in the possession of ThyssenKrupp and is subject to further breaches so long as ThyssenKrupp fails to undertake appropriate measures to protect the PII in their possession; and

i. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

58. The value of Plaintiffs' and the Class Members' PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" Internet websites, making the information publicly available, for a substantial fee of course.

59. It can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash. That is precisely what makes PII more desirable to criminals than credit card theft. Credit card theft can be spotted by banks early on, and accounts can be

quickly frozen or cancelled once the fraud is detected, making credit card data much less valuable to criminals than PII.

60. ThyssenKrupp disclosed the PII of Plaintiffs and the Class Members for criminals to use in the conduct of criminal activity. Specifically, ThyssenKrupp opened up, disclosed, and exposed the PII of Plaintiffs and the Class Members to persons engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen PII.

61. ThyssenKrupp's use of outdated and unsecured computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for healthcare employee privacy, and has exposed the PII of Plaintiffs and thousands of Class Members to unscrupulous operators, con artists, and outright criminals.

PLAINTIFFS' EXPERIENCE

62. Plaintiff Darnell Crawford is a truck driver for ThyssenKrupp who is a citizen of Missouri.

63. Due to the risk of fraudulent activity that Mr. Crawford has been exposed to, he has been forced to subscribe to identity theft protection with LifeLock into the foreseeable future.

64. To Mr. Crawford's knowledge, his PII has never been compromised in a data breach before.

65. Plaintiff Michael Dew is also a truck driver for ThyssenKrupp who is a citizen of Missouri.

66. Shortly after the Data Breach, Mr. Dew noticed fraudulent activity on the checking account that he used for direct deposit with ThyssenKrupp.

67. Due to the fraudulent activity that Mr. Dew experienced, he has been forced to subscribe to identity theft protection with LifeLock into the foreseeable future.

68. To Mr. Dew's knowledge, his PII has never been compromised in a data breach before.

69. As a condition for attaining employment with ThyssenKrupp, Plaintiffs and class members were required to make available to ThyssenKrupp, its agents, and its employees, sensitive and confidential PII, including, but not limited to, names, dates of birth, addresses, Social Security numbers, direct deposit information, payroll information, health information, and contact information.

70. ThyssenKrupp acquires, collects, and stores a massive amount of PII from its employees.

71. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' PII, and by storing it in a fashion where it can easily become compromised, ThyssenKrupp assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting its employees' PII from unauthorized disclosure.

72. Plaintiffs have taken reasonable steps to maintain the confidentiality of their PII.

73. Plaintiffs relied on ThyssenKrupp to keep their PII confidential and securely maintained, to use this information for business purposes only, and to take reasonable steps to ensure that ThyssenKrupp's vendors would make only authorized disclosures of that information.

74. Plaintiffs entrusted their PII to ThyssenKrupp solely for the purpose of attaining employment with the expectation and implied mutual understanding that ThyssenKrupp would strictly maintain the confidentiality of the PII and safeguard it from theft or misuse.

75. Plaintiffs would not have entrusted ThyssenKrupp with their PII had they known ThyssenKrupp would fail to take adequate steps to secure its computer and email systems.

76. Plaintiffs received a letter from ThyssenKrupp (the "Notice Letter") notifying them of the Data Breach. The Notice Letter informed them that they were a victim of the Data Breach and that their PII was compromised.

77. As a result of the Data Breach, Plaintiffs must expend considerable time and effort monitoring their accounts to protect themselves from additional identity theft.

78. Aside from the financial loss consequences, both direct and indirect, that Plaintiffs are more than likely to face, identity theft negatively impacts credit scores.[20] Because a criminal's delinquent payments, cash loans, or even foreclosures slowly manifest into weakened credit scores, and because this type of fraud takes the longest time to resolve, Plaintiffs were forced to subscribe to a credit monitoring service for the indefinite future.

79. It can take years to spot identity or PII theft. Even if ThyssenKrupp offered Plaintiffs a lifetime subscription to a credit monitoring service, Plaintiffs would be powerless to prevent identity theft.

80. As previewed above, as the amount of information from both unregulated sources that have identities and addresses attached (*i.e.*, phone books, search engines, and websites) and

[20] Direct financial loss refers to the amount of money stolen or misused by the identity theft offender. Indirect financial loss includes any outside costs associated with identity theft, like legal fees or overdraft charges. A 2014 Department of Justice study found that victims experienced a combined average loss of $1,343.00. In total, identity theft victims lost a whopping $15.4 billion in 2014 alone. *See* Gredler, Cody, *The Real Cost of Identity Theft*, CSIDENTITY, (Sep. 9, 2016), https://www.csid.com/2016/09/real-cost-identity-theft/ (last visited March 26, 2020).

illegal sources (*i.e.*, stolen information like the PII) grows over time, there is more and more information about who people might be. As a result, cyber-criminals can cross-reference these two sources to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.[21]

81. These techniques mean that the PII stolen in the Data Breach can easily be used to link and identify it to Plaintiffs' and the Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even though certain information such as emails, phone numbers or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, they can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what has happened or is likely to happen to Plaintiffs and the Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to so find.

82. Identity theft is not only impacting Plaintiffs and Class Members financially, but it is taking a significant emotional and physical toll. Plaintiffs and other Class Members, like other

[21] "Fullz" is fraudster speak for data that includes the *full* information of the victim, including name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), *available at* https://krebsonsecurity.com/tag/fullz/ (last visited March 26, 2020).

PII theft victims, fear for their personal financial security and are experiencing feelings of rage and anger, anxiety, sleep disruption, stress, fear, and physical pain.

83. This goes far beyond allegations of mere worry or inconvenience; the injury and harm to a Data Breach victim is the type contemplated and addressed by law.

CLASS ALLEGATIONS

84. Pursuant to Missouri Court Rule of Civil Procedure 52.08, Plaintiffs brings this class action on behalf of themselves and the following proposed Class (the "Class"):

> All citizens of Missouri whose PII was compromised as a result of the Data Breach with ThyssenKrupp which was announced by ThyssenKrupp on January 28, 2021.

85. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which the Defendants or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

86. Plaintiffs and the Class Members satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Rule 52.08(a).

87. **Numerosity**: The exact number of Class members is unknown but is estimated to be at least 4,000 persons at this time, and individual joinder in this case is impracticable. Class Members can be easily identified through Defendants' records and objective criteria permitting

self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies**.**

88. **Typicality**: Plaintiffs' claims are typical of the claims of other Class members in that Plaintiffs, and the Class Members sustained damages arising out of Defendants' Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiffs and the Class Members sustained similar injuries and damages, as a result of Defendants' uniform illegal conduct.

89. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiffs have no interests that conflict with, or are antagonistic to those of, the Class, and Defendants have no defenses unique to Plaintiffs.

90. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

a. whether Defendants violated the laws asserted herein, and other statutory privacy laws;

b. whether Defendants had a duty to use reasonable care to safeguard Plaintiffs' and the Class Members' PII;

c. whether Defendants breached the duty to use reasonable care to safeguard Class Members' PII;

d. whether Defendants breached its contractual promises to safeguard Plaintiffs' and the Class Members' PII;

e. whether Defendants was negligent *per se* in not complying with privacy laws;

f. whether Defendants knew or should have known its practices and representations related to the Notice Letter, Data Breach, and PII were deceptive and unfair;

g. whether Defendants knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PII;

h. whether Defendants failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and the other Class Members' PII from unauthorized release and disclosure;

i. whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendants' computer and software systems to safeguard and protect Plaintiffs' and the other Class Members' PII from unauthorized release and disclosure;

j. whether Defendants took reasonable measures to determine the extent of the Data Breach after it was discovered;

k. whether Defendants' delay in informing Plaintiffs and the other Class Members of the Data Breach was unreasonable;

l. whether Defendants' method of informing Plaintiffs and the other Class Members of the Data Breach was unreasonable;

m. whether Defendants' conduct was likely to deceive the public;

n. whether Defendants is liable for negligence or gross negligence;

o. whether Defendants' conduct, practices, statements, and representations about the Data Breach of the PII violated applicable state laws;

p. whether Defendants knew or should have known its representations were false, deceptive, unfair, and misleading;

q. whether Plaintiffs and the Class Members were injured as a proximate cause or result of the Data Breach;

r. whether Plaintiffs and the Class Members were damaged as a proximate cause or result of Defendants' breach of its contract with Plaintiffs and the Class Members;

s. whether Defendants' practices and representations related to the Data Breach that compromised the PII breached implied warranties;

t. what the proper measure of damages is; and

u. whether Plaintiffs and the Class Members are entitled to restitutionary, injunctive, declaratory, or other relief.

91. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties

and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered, and uniformity of decisions ensured.

92. A class action is therefore superior to individual litigation because:

a. the amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendants' conduct economically feasible in the absence of the class action procedural device;

b. individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

93. In addition to satisfying the prerequisites of Rule 52.08(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 52.08(b) because:

a. the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendants;

b. the prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

c. Defendants has acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief herein appropriate with respect to the proposed Class as a whole.

d. questions of law or fact common to the members of the class predominate over any questions affecting only individual members, and that a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

COUNT I
Negligence
On Behalf of Plaintiffs and the Class against Defendants

94. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

95. Plaintiffs and Class Members entrusted their PII to Defendants. Defendants owed to Plaintiffs and the other Class Members a duty to exercise reasonable care in handling and using the PII in their care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

96. Defendants owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendants' failure to adequately safeguard PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass and the two ransomware attacks that preceded it. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the manner in which the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

97. Defendants owed to Plaintiffs and the Class Members a duty to notify them within a reasonable time frame of any breach to the security of their PII under Mo. Stat. § 407.1500 *et seq.* and other laws as referred to herein. Defendants also owed a duty to timely and accurately disclose to Plaintiffs and the other Class Members the scope, nature, and occurrence of the Data Breach. This duty is required and necessary in order for Plaintiffs and the other Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

98. Defendants owed these duties to Plaintiffs and the other Class Members because they are members of a well-defined, foreseeable, and probable class of individuals who Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Plaintiffs and the other Class Members were required to provide their personal information and PII to Defendants in order to work for it, and Defendants retained the information throughout Plaintiffs' and the other Class Members' employment there.

99. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. As the holder of vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PII—whether by phishing or otherwise. Especially, given the fact that ThyssenKrupp was the victim of two other ransomware attacks shortly before the Data Breach.

100. Defendants breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and the other Class Members which actually and proximately caused the Data Breach and Plaintiffs' and the other Class Members' injury. Defendants further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs

and the other Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and the other Class Members' injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

101. Defendants' breach of its common law duties to exercise reasonable care and its failures and negligence actually and proximately caused the Plaintiffs' and other Class Members' actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted and was caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
On Behalf of Plaintiffs and the Class against Defendants

102. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

103. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

104. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect employees' PII. The FTC publications

and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiffs' and Class Members' sensitive PII.

105. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect employees' PII and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of employee PII it collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to employees in the event of a breach, which ultimately came to pass—like the two other ransomware attacks that happened shortly before the Data Breach.

106. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm to its employees as that suffered by Plaintiffs and the Class Members.

107. Defendants had a duty to Plaintiffs and Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII.

108. Defendants breached its respective duties to Plaintiffs and the Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

109. Defendants' violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

110. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, they would not have been injured.

111. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that Defendants was failing to meet its duties and that its breach would cause Plaintiffs and Class Members to suffer the foreseeable harms associated with the exposure of their PII.

112. Had Plaintiffs and the Class members known that Defendants did not adequately protect employee PII, they would not have entrusted Defendants with their PII.

113. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Invasion of Privacy
On Behalf of Plaintiffs and the Class against Defendants

114. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

115. Defendants publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiffs and Class Members by disclosing and exposing Plaintiffs' and Class Members' PII to enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the dark web and elsewhere.

116. That is so, simply because the NetWalker ransomware group published Plaintiffs' and Class Members' PII online as part of its ransomware strategy.

117. The disclosure of the PII, including employees' names, addresses, dates of birth, Social Security numbers, direct deposit information, payroll information, health information, and contact information is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

118. Defendants has a special relationship with Plaintiffs and the Class Members and Defendants' disclosure of PII is certain to embarrass them and offend their dignity. Defendants should appreciate that the cyber-criminals who stole the PII would further sell and disclose the PII as they are doing. That the original disclosure is devastating to the Plaintiffs and the Class Members, even though it originally may have only been disclosed to one person or a limited number of cyber-criminals, does not render it any less a disclosure to the public-at-large.

119. The tort of public disclosure of private facts is recognized in Missouri. *See Sullivan v. Pulitzer Broad. Co.*, 709 S.W.2d 475 (Mo. 1986). Plaintiffs' and the Class Members' PII was publicly disclosed by Defendants in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendants knew that Plaintiffs' and Class Members' PII is not a matter of legitimate public concern. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been injured and are entitled to damages.

COUNT IV
Breach of Contract against Defendants
On Behalf of Plaintiffs and the Class

120. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

121. Defendants offered Plaintiffs and Class Members employment, which they accepted by reporting to work under no obligation to do so.

122. The agreement was supported by adequate consideration because Defendants remunerated the Class Members for their labor.

123. Plaintiffs and the members of the Class provided their PII in connection with their employment with Defendants in order to verify their identity, receive compensation and in order for Defendants to have complete employee records for tax purposes, amongst other things.

124. Plaintiffs and the members of the Class provided various sensitive and personal information to Defendants as a condition precedent to their employment with Defendants, or in connection with employer sponsored benefits.

125. Understanding the sensitive nature of the PII, Defendants implicitly promised Plaintiffs and the class members that they would take adequate measures to protect their sensitive and personal information.

126. A material term of this agreement is a covenant by Defendants that they will take reasonable efforts to safeguard that information.

127. Plaintiffs and the Class Members relied upon that covenant and would not have disclosed their PII without assurances that it would be properly safeguarded. Moreover, the covenant to adequately safeguard the PII is an implied term, to the extent it is not an express term.

128. Plaintiffs and the class members fulfilled their obligations under the contract by providing their PII to Defendants.

129. Defendants, however, failed to safeguard and protect the PII. Defendants' breach of its obligations under the contract between the parties directly caused Plaintiffs and the class members to suffer injuries.

130. Defendants materially breached the express or implied contract(s) it had entered with Plaintiffs and Class Members by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendants further breached the implied contracts with Plaintiffs and Class members by:

a. Failing to properly safeguard and protect Plaintiffs' and Class Members' PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement.

131. The damages sustained by Plaintiffs and Class Members as described above were the direct and proximate result of Defendants' material breaches of its agreements.

132. Plaintiffs and Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendants.

133. Under the laws of Missouri, good faith is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

134. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

135. Defendants failed to promptly advise Plaintiffs and Class Members of the Data Breach.

136. In these and other ways, Defendants violated its duty of good faith and fair dealing.

137. Plaintiffs and Class Members have sustained damages as a result of Defendants' breaches of its agreements, including breaches thereof through violations of the covenant of good faith and fair dealing.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Class, requests that the Court:

A. Certify this case as a Class action on behalf of the Class defined above, appoint Plaintiffs Darnell Crawford and Michael Dew as Class representatives, and appoint the undersigned as Class counsel;

B. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class Members;

C. Award injunctive relief as is necessary to protect the interests of Plaintiffs and the Class Members;

D. Enter an award in favor of Plaintiffs and the Class Members that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

E. Award restitution and damages to Plaintiffs and the Class Members in an amount to be determined at trial;

F. Enter an award of attorneys' fees and costs, as allowed by law;

G. Enter an award of pre-judgment and post-judgment interest, as provided by law;

H. Grant Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Grant such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: February 25, 2021

Respectfully submitted,

/s/John F. Garvey

John F. Garvey #35879
CAREY DANIS & LOWE
8235 Forsyth Blvd., Ste. 1100
St. Louis, MO 63105
Tel: (314) 725-7700
Fax: (314) 678-3401
jgarvey@careydanis.com

Aaron Haber, Esq. #57449
MUCHNICK HABER MARGOLIS, LC
8151 Clayton Rd., Ste. 201
Clayton, MO 63117
Tel: (314) 725-5050
Fax: (314) 726-2042
aaron@mhmlegal.com

Lynn A. Toops
Lisa M. La Fornara
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

J. Gerard Stranch, IV*
Peter J. Jannace*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
peterj@bsjfirm.com

*Motion for admission to be filed

Counsel for Plaintiff and the Proposed Class

Certificate of Filing

The undersigned hereby certifies that the foregoing Class Action Petition has been filed by using the Court's Electronic Case Filing system on this 25th day of February, 2021.

/s/John F. Garvey

IN THE CIRCUIT COURT OF THE CITY OF ST. LOUIS
STATE OF MISSOURI

DARNELL CRAWFORD, *et al.*, *Plaintiffs,* **VS.** **THYSSENKRUPP MATERIALS NA, INC.,** *et al.*, *Defendant*,	)	**CASE NO. 2122-CC00411**

CERTIFICATE OF SERVICE

The undersigned hereby certifies that Plaintiffs' First Eleven (11) Interrogatories Directed to Defendant ThyssenKrupp Materials NA, Inc. and Plaintiffs' First Nineteen (19) Requests for Production of Documents and Things Directed to Defendant ThyssenKrupp Materials NA, Inc. were provided to the process server on this 4th day of March, 2021, for service at the time of and simultaneously along with service of the Summons and Class Action Petition on said Defendant at the following address:

ThyssenKrupp Materials NA, Inc.
C/O CSC-Lawyers Incorporating Service Company
221 Bolivar Street
Jefferson City, MO 65101
Defendant.

Respectfully submitted,

/s/John F. Garvey

John F. Garvey #35879
CAREY DANIS & LOWE
8235 Forsyth Blvd., Ste. 1100
St. Louis, MO 63105
Tel: (314) 725-7700
Fax: (314) 678-3401
jgarvey@careydanis.com

Aaron Haber, Esq. #57449
MUCHNICK HABER MARGOLIS, LC
8151 Clayton Rd., Ste. 201
Clayton, MO 63117
Tel: (314) 725-5050
Fax: (314) 726-2042
aaron@mhmlegal.com

Lynn A. Toops
Lisa M. La Fornara
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

J. Gerard Stranch, IV*
Peter J. Jannace*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
peterj@bsjfirm.com

*Motion for admission to be filed

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Certificate of Service has been filed by using the Court's Electronic Case Filing System on this 4th day of March, 2021.

/s/John F. Garvey
John F. Garvey- 35879

IN THE CIRCUIT COURT OF THE CITY OF ST. LOUIS
STATE OF MISSOURI

DARNELL CRAWFORD, *et al.*, *Plaintiffs,* **VS.** **THYSSENKRUPP MATERIALS NA, INC.,** *et al.*, *Defendant*,	)	**CASE NO. 2122-CC00411**

CERTIFICATE OF SERVICE

The undersigned hereby certifies that Plaintiffs' First Eleven (11) Interrogatories Directed to Defendant ThyssenKrupp Supply Services NA, Inc. and Plaintiffs' First Nineteen (19) Requests for Production of Documents and Things Directed to defendant ThyssenKrupp Supply Services NA, Inc. were provided to the process server on this 4th day of March, 2021, for service at the time of and simultaneously along with service of the Summons and Class Action Petition on said Defendant at the following address:

ThyssenKrupp Supply Chain Services NA, Inc.
C/O CSC-Lawyers Incorporating Service Company
221 Bolivar Street
Jefferson City, MO 65101
Defendant.

Respectfully submitted,

/s/John F. Garvey

John F. Garvey #35879
CAREY DANIS & LOWE
8235 Forsyth Blvd., Ste. 1100
St. Louis, MO 63105
Tel: (314) 725-7700
Fax: (314) 678-3401
jgarvey@careydanis.com

Aaron Haber, Esq. #57449
MUCHNICK HABER MARGOLIS, LC
8151 Clayton Rd., Ste. 201
Clayton, MO 63117
Tel: (314) 725-5050
Fax: (314) 726-2042
aaron@mhmlegal.com

Lynn A. Toops
Lisa M. La Fornara
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

J. Gerard Stranch, IV*
Peter J. Jannace*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
peterj@bsjfirm.com

*Motion for admission to be filed

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Certificate of Service has been filed by using the Court's Electronic Case Filing System on this 4th day of March, 2021.

/s/John F. Garvey
John F. Garvey- 35879

IN THE CIRCUIT COURT OF THE CITY OF ST. LOUIS
STATE OF MISSOURI

DARNELL CRAWFORD, *et al.*, *Plaintiffs,* **VS.** **THYSSENKRUPP MATERIALS NA, INC.,** *et al.*, *Defendant*,	)	**CASE NO. 2122-CC00411**

MEMORANDUM FILING RETURN OF SERVICE ON DEFENDANT THYSSENKRUPP MATERIALS NA, INC.

Come now Plaintiffs and file herewith Affidavit of Service on Defendant ThyssenKrupp Materials NA, Inc. Defendant was served on March 4, 2021.

Respectfully submitted,

/s/John F. Garvey

John F. Garvey #35879
CAREY DANIS & LOWE
8235 Forsyth Blvd., Ste. 1100
St. Louis, MO 63105
Tel: (314) 725-7700
Fax: (314) 678-3401
jgarvey@careydanis.com

Aaron Haber, Esq. #57449
MUCHNICK HABER MARGOLIS, LC
8151 Clayton Rd., Ste. 201
Clayton, MO 63117
Tel: (314) 725-5050
Fax: (314) 726-2042
aaron@mhmlegal.com

Lynn A. Toops
Lisa M. La Fornara
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

J. Gerard Stranch, IV*
Peter J. Jannace*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
peterj@bsjfirm.com

*Motion for admission to be filed

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Memorandum Filing Return of Service has been filed by using the Court's Electronic Case Filing System on this 12th day of March, 2021.

/s/John F. Garvey
John F. Garvey- 35879

IN THE 22ND JUDICIAL CIRCUIT, CITY OF ST LOUIS, MISSOURI

Judge or Division: MICHAEL FRANCIS STELZER	**Case Number: 2122-CC00411**	
Plaintiff/Petitioner: DARNELL CRAWFORD JR vs.	Plaintiff's/Petitioner's Attorney/Address JOHN FRANCIS GARVEY JR 4455 RIDGEWOOD AVE PO BOX 22139 SAINT LOUIS, MO 63116	
Defendant/Respondent: THYSSENKRUPP MATERIALS NA, INC	Court Address: CIVIL COURTS BUILDING 10 N TUCKER BLVD SAINT LOUIS, MO 63101	(Date File Stamp)
Nature of Suit: CC Other Tort		

Summons in Civil Case

The State of Missouri to: THYSSENKRUPP MATERIALS NA, INC
Alias:

CSC LAWYERS INC SERVICE
COMPANY 221 BOLIVAR STREET
JEFFERSON CITY, MO 65101

COLE COUNTY, MO

COURT SEAL OF
CITY OF ST LOUIS

You are summoned to appear before this court and to file your pleading to the petition, a copy of which is attached, and to serve a copy of your pleading upon the attorney for plaintiff/petitioner at the above address all within 30 days after receiving this summons, exclusive of the day of service. If you fail to file your pleading, judgment by default may be taken against you for the relief demanded in the petition.

March 4, 2021
Date

Thomas Klepfinger
Clerk

Further Information:

Sheriff's or Server's Return

Note to serving officer: Summons should be returned to the court within 30 days after the date of issue.

I certify that I have served the above summons by: (check one)

☐ delivering a copy of the summons and a copy of the petition to the defendant/respondent.

☐ leaving a copy of the summons and a copy of the petition at the dwelling place or usual abode of the defendant/respondent with _____, a person of the defendant's/respondent's family over the age of 15 years who permanently resides with the defendant/respondent.

☒ (for service on a corporation) delivering a copy of the summons and a copy of the complaint to: Lauren Shipley (name) Authorized Agent (title).

☐ other: _____.

Served at 221 Bolivar St. Jefferson City MO (address)

in Cole (County/City of St. Louis), MO, on 3-4-21 (date) at 2:20 pm (time).

Rufus R. Harmon
Printed Name of Sheriff or Server

Rufus R. Harmon
Signature of Sheriff or Server

Must be sworn before a notary public if not served by an authorized officer:

Subscribed and sworn to before me on 03-08-2021 (date).

My commission expires: 03-03-2025
Date

Donna R. Meyr
Notary Public

Donna R. Meyr
Notary Public-Notary Seal
STATE OF MISSOURI
Commissioned for Cole County
My Commission Expires: March 3, 2025
ID: 13435325

Sheriff's Fees, if applicable

Summons	$_____
Non Est	$_____
Sheriff's Deputy Salary Supplemental Surcharge	$ 10.00
Mileage	$_____ (_____ miles @ $._____ per mile)
Total	$_____

A copy of the summons and a copy of the petition must be served on each defendant/respondent. For methods of service on all classes of suits, see Supreme Court Rule 54.

Donna R. Meyr
Notary Public-Notary Seal
STATE OF MISSOURI
Commissioned for Cole County
My Commission Expires: March 3, 2025
ID. #13435325

HARMON LEGAL PROCESS SERVICI
P.O. Box 1794
Jefferson City, MO 65102-1794
Phone: (573) 635-6690
Fax: (573) 635-2339
46-3172219

INVOICE

Invoice #RRH-2021000405
3/4/2021

Lori Eyre
CAREY DANIS & LOWE
8235 Forsyth
Ste. 1100
St. Louis, MO 63105

Case Number: St. Louis City 2122-CC00411

Plaintiff:
DARNELL CRAWFORD, JR.

Defendant:
THYSSENKRUPP MATERIALS NA, INC.

Served: 3/4/2021 2:20 pm
To be served on: Thyssenkrupp Materials Na, Inc., c/o CSC

ITEMIZED LISTING

Line Item	Quantity	Price	Amount
Service of Summons in Jefferson City, Mo.	1.00	50.00	50.00
TOTAL CHARGED:			$50.00
BALANCE DUE:			**$50.00**

Please enclose a copy of this invoice with your payment.

IN THE CIRCUIT COURT OF THE CITY OF ST. LOUIS
STATE OF MISSOURI

DARNELL CRAWFORD, *et al.*, *Plaintiffs,* **VS.** **THYSSENKRUPP MATERIALS NA, INC.,** *et al.*, *Defendant*,	)	**CASE NO. 2122-CC00411**

MEMORANDUM FILING RETURN OF SERVICE
ON DEFENDANT THYSSENKRUPP SUPPLY CHAIN SERVICES NA, INC.

Come now Plaintiffs and file herewith Affidavit of Service on Defendant ThyssenKrupp Supply Chain NA, Inc. Defendant was served on March 4, 2021.

Respectfully submitted,

/s/John F. Garvey

John F. Garvey #35879
CAREY DANIS & LOWE
8235 Forsyth Blvd., Ste. 1100
St. Louis, MO 63105
Tel: (314) 725-7700
Fax: (314) 678-3401
jgarvey@careydanis.com

Aaron Haber, Esq. #57449
MUCHNICK HABER MARGOLIS, LC
8151 Clayton Rd., Ste. 201
Clayton, MO 63117
Tel: (314) 725-5050
Fax: (314) 726-2042
aaron@mhmlegal.com

Lynn A. Toops
Lisa M. La Fornara
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

J. Gerard Stranch, IV*
Peter J. Jannace*
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gerards@bsjfirm.com
peterj@bsjfirm.com

*Motion for admission to be filed

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Memorandum Filing Return of Service has been filed by using the Court's Electronic Case Filing System on this 12th day of March, 2021.

/s/John F. Garvey
John F. Garvey- 35879

IN THE 22ND JUDICIAL CIRCUIT, CITY OF ST LOUIS, MISSOURI

Judge or Division: MICHAEL FRANCIS STELZER	**Case Number: 2122-CC00411**	
Plaintiff/Petitioner: DARNELL CRAWFORD JR vs.	Plaintiff's/Petitioner's Attorney/Address JOHN FRANCIS GARVEY JR 4455 RIDGEWOOD AVE PO BOX 22139 SAINT LOUIS, MO 63116	
Defendant/Respondent: THYSSENKRUPP MATERIALS NA, INC	Court Address: CIVIL COURTS BUILDING 10 N TUCKER BLVD SAINT LOUIS, MO 63101	(Date File Stamp)
Nature of Suit: CC Other Tort		

Summons in Civil Case

The State of Missouri to: THYSSENKRUPP SUPPLY CHAIN SERVICES NA, INC.
Alias:

CSC LAWYERS INCORPORATING
SERVICE COMPANY
221 BOLIVAR STREET
JEFFERSON CITY, MO 65101

COLE COUNTY, MO

COURT SEAL OF
CIRCUIT COURT OF MISSOURI
CITY OF ST LOUIS

You are summoned to appear before this court and to file your pleading to the petition, a copy of which is attached, and to serve a copy of your pleading upon the attorney for plaintiff/petitioner at the above address all within 30 days after receiving this summons, exclusive of the day of service. If you fail to file your pleading, judgment by default may be taken against you for the relief demanded in the petition.

March 4, 2021
Date

Thomas Kloeppinger
Clerk

Further Information:

Sheriff's or Server's Return

Note to serving officer: Summons should be returned to the court within 30 days after the date of issue.

I certify that I have served the above summons by: (check one)

☐ delivering a copy of the summons and a copy of the petition to the defendant/respondent.

☐ leaving a copy of the summons and a copy of the petition at the dwelling place or usual abode of the defendant/respondent with _____, a person of the defendant's/respondent's family over the age of 15 years who permanently resides with the defendant/respondent.

☒ (for service on a corporation) delivering a copy of the summons and a copy of the complaint to: Lauren Shipley (name) Authorized Agent (title).

☐ other: _____.

Served at 221 Bolivar St. Jefferson City MO (address)
in Cole (County/City of St. Louis), MO, on 3-4-21 (date) at 2:20 p.m. (time).

Rufus R. Harmon
Printed Name of Sheriff or Server

Rufus R. Harmon
Signature of Sheriff or Server

Donna R. Meyer
Notary Public-Notary Seal
STATE OF MISSOURI
Commissioned for Cole County
My Commission Expires: March 3, 2025
ID. #13435325

Must be sworn before a notary public if not served by an authorized officer:

Subscribed and sworn to before me on 03-08-2021 (date).

My commission expires: 03-03-2025
Date

Donna R. Meyer
Notary Public

Sheriff's Fees, if applicable

Summons	$_____
Non Est	$_____
Sheriff's Deputy Salary Supplemental Surcharge	$ 10.00
Mileage	$_____ (_____ miles @ $._____ per mile)
Total	$_____

A copy of the summons and a copy of the petition must be served on **each** defendant/respondent. For methods of service on all classes of suits, see Supreme Court Rule 54.

HARMON LEGAL PROCESS SERVICI
P.O. Box 1794
Jefferson City, MO 65102-1794
Phone: (573) 635-6690
Fax: (573) 635-2339
46-3172219

INVOICE

Invoice #RRH-2021000406
3/4/2021

Lori Eyre
CAREY DANIS & LOWE
8235 Forsyth
Ste. 1100
St. Louis, MO 63105

Case Number: St. Louis City 2122-CC00411

Plaintiff:
DARNELL CRAWFORD, JR.

Defendant:
THYSSENKRUPP MATERIALS NA, INC.

Served: 3/4/2021 2:20 pm
To be served on: Thyssenkrupp Supply Chain Services NA, Inc., c/o CSC

ITEMIZED LISTING

Line Item	Quantity	Price	Amount
Service of Summons in Jefferson City, Mo.	1.00	30.00	30.00
TOTAL CHARGED:			$30.00
BALANCE DUE:			**$30.00**

Please enclose a copy of this invoice with your payment.

IN THE CIRCUIT COURT OF THE CITY OF ST. LOUIS
STATE OF MISSOURI

DARNELL CRAWFORD, ET AL.,	)	
	)	
Plaintiffs,	)	
	)	Case No. 2122-CC00411
v.	)	
	)	
THYSSENKRUPP MATERIALS, NA., INC.,	)	
	)	
	)	
Defendants.	)	

ENTRY OF APPEARANCE

COMES NOW Aaron D. Haber of Muchnick Haber Margolis, LC, and hereby enters his appearance on behalf of Plaintiffs Darnell Crawford and Michael Dew as co-counsel in the above-referenced case.

MUCHNICK HABER MARGOLIS, LC

By: /s/ Aaron D. Haber

AARON D. HABER, #57449
Attorney for Plaintiffs
8151 Clayton Road, Suite 201
St. Louis, Missouri 63117
(314) 725-5050 (telephone)
(314) 726-2042 (facsimile)
aaron@mhmlegal.com